Before the

FEDERAL COMMUNICATIONS COMMISSION

Washington, D.C. 20554

In the Matter of	)	
	)	
IP-Enabled Services	)	W.C. Docket No. 04-36

Nortel Networks

Appendix 2: The Network Transformation

May 28, 2004

For many years, service providers have enjoyed solid revenue streams from their voice, private line, and switched data businesses while supporting the less profitable, but emerging IP data transport business. Meanwhile, IP traffic volumes increased at exponential rates. In 2002, IP revenue-bearing traffic displaced voice traffic as the largest volume component of carrier networks,[1] yet it continues to generate less than ten percent of all service provider revenue. The implications of this shift cannot be overstated, and service providers consequently have been faced with the re-evaluation of their entire business model.

Other changes have gone hand in hand with the dominance of IP. The strong business case for migrating voice to a packet-based network has led to a convergence of voice and data networks to a single packet infrastructure. The trend to carry ever more

[1] Ryan Hankin Kent, Telecom Economics Market Update, August 2003.

essential services over packet networks has generated a need for an IP network that is more robust, secure, and scalable than conventional router technology can deliver. In addition, a growing mix of hosted and managed services over a single network has generated requirements for service differentiation that are best addressed by adding intelligence to the network.

The changes that are reverberating through the communications network industry are too profound and far-reaching to be solved by patchwork solutions. They require nothing less than a complete transformation of the service provider business model, and a corresponding transformation of the underlying networks. This network transformation will encompass three key requirements: network convergence, carrier grade performance, and service intelligence. The result will be a packet network that is far more intelligent, reliable, secure, scalable, manageable, and efficient than today's router-based IP networks.

Network Convergence

The communications services that we use today in our homes, our cars, and our businesses are delivered by several different networks, each of which is designed to deliver one type of service. The result is a web of overlay networks that all touch the same consumers. For example, a typical residential consumer subscribes to home telephone service, cell phone service, Internet service, and cable television, each of which – even when delivered by a single service provider – resides on a different network. These parallel networks are costly to operate, difficult to maintain, and often lack scalability.

Network convergence eliminates the multiplicity of networks and is an important step toward the transformation of the service provider business model. A converged network will incur lower operating and capital expenditures, enable innovative new IP services, be responsive to centralized management, and will use capacity more efficiently than do fragmented networks. The converged networks will deliver services intelligently, while being simple to use and to manage.

Convergence of voice and data networks

The packetization of voice has passed the early-adopter phase and is addressing the needs of the mass market, with large-scale deployments underway with Verizon, Sprint, Cox Communications, and many others. The appeal of new revenue opportunities combined with reductions in capital and operating expense is driving this powerful movement. The result will be a far simpler network with smaller footprint, greater scalability, and the ability to deliver value-rich, multimedia services.

Convergence of the network edge

Different types of packet networks have evolved over time to support different types of traffic.

- ATM and Frame Relay networks support business needs with a high level of reliability, security, and predictability.
- IP networks support ubiquitous connectivity over the popular IP protocol.
- Optical networks deliver enormous bandwidth with low administrative overhead as well as leased line services.

These networks coexist at different "layers" of the network hierarchy, and the boundaries between them are fading with the broad acceptance of hybrid protocols such as Multi-Protocol Label Switching (MPLS), which support multiple traffic types over an optical backbone.

The network edge is the focal point for efficiently converging many types of traffic and access types onto one packet core network.

Convergence of wireline and wireless network

Global standards are being defined that increasingly lay the groundwork for a single network with the capabilities to support all types of traffic at today's performance levels. As with the wireline network, wireless voice traffic is becoming increasingly packet-based, as 3G networks become the industry standard worldwide. The rationale that once existed for having separate wireline and wireless networks fades as all traffic on both networks becomes packet-based and uses the same network protocols.

Network convergence will be an important step on the road to network transformation. It will free service providers from the costly necessity of maintaining and growing numerous parallel networks. But more importantly, the converged network will lay the foundation for innovative new IP-enabled services that can be developed, deployed, and provisioned quickly, and managed centrally.

Carrier Grade Performance

Multiple traditional service provider networks are converging into a much smaller number of packet-based networks. Clearly, not all of today's networks operate with the same levels of security, dependability, or manageability. The converged network will carry mission-critical data traffic alongside latency-sensitive voice/video traffic and bursty high-volume traffic such as storage back-ups. It must have the robustness and security to satisfy the requirements of each traffic type and of the consumers using them. In short, the transformed network must be carrier grade.

The term carrier grade is broad. In additional to traditional requirements such as scalability and back-office integration, there are three requirements for carrier grade networks.

Network dependability

With a network outage costing as much as $6 million per hour,[2] dependability is the most universally recognized carrier grade requirement. Historically, dependability is synonymous with hardware reliability – but the move to converged networks will change how we think about the network as a whole.

The new standard for product dependability, incorporating both hardware and software, is "six-9s," or 30 seconds of downtime per year.

But network dependability encompasses more than just products. The network must continue to operate even when portions of it are unavailable due to a power outage or when network upgrades require that intermediate equipment be taken out of service. Total network dependability includes two additional critical factors: support for network protocols that quickly discover alternate paths to the intended destination, and proper network design that allows these protocols to provide the highest level of dependability at the lowest reasonable cost.

Secure networking

As is the case with dependability, convergence expands the requirements for securing service provider networks. The move to converged packet networks – where control traffic shares the same bandwidth with user information – exposes broad

[2] Contingency Planning Research, http://www.contingencyplanning research.com/cod.htm, 1996

segments of the public network to attacks from literally millions of places and users. The network and its components must be designed to ensure the availability of the infrastructure as well as the integrity of the subscriber data.

In addition to having appropriate procedures and user training, building a secure network requires integrating best practices into every phase of the product lifecycle. The product must be designed and built with security in mind, or exceeding a baseline of industry-standard security specifications from such bodies as ANSI, Optical Interoperability Forum, CTIA, and the U.S. National Security Telecommunications Advisory Committee (NSTAC). A comprehensive testing process is necessary to ensure that each product is protected from known forms of attack, and equipment suppliers must be prepared to respond to newly discovered vulnerabilities.

Investment Protection

Migrating to a converged network only makes sense when it makes good business sense for service providers, and such a migration only makes sense when it is transparent to the end-user. The new network must provide the same capabilities as the existing voice network – from E911 to Centrex. And, of course, it must be as manageable and as scalable as the network it replaces.

Carrier grade performance is not just about building products with high reliability; it is about building a network that will deliver better-than-voice-grade service with full security and availability despite disasters, attacks, overloads, or errors.

Service Intelligence

As networks converge and carrier grade performance becomes a basic requirement, the emphasis moves to enabling the IP-enabled services that will drive service provider profitability and ensure that consumers have access to such services. Tomorrow's network will be expected to rigorously fulfill customer service expectations and to deliver on bandwidth commitments and quality of service guarantees.

The attribute that will enable the network to fulfill these expectations is service intelligence. Service intelligence simplifies the process of creating, integrating, and offering new services, while adding new levels of service awareness for the converged network. This makes the network more than just the sum of its parts. The service-intelligent network will have the ability to act as one cohesive network rather than a collection of network elements that must be individually managed and programmed, as frequently has been the case in the pact.

Today's networks have a limited amount of intelligence – an ability to prioritize and shape traffic based on pre-defined criteria, for example. Service intelligence goes beyond this, enabling the service provider to easily provide triple play services – for example, based on *who the user is* and *how he/she is connected* to the network. Service intelligence capabilities include the following:

Application awareness

The network must understand the requirements of each application and respond appropriately. For example, voice calls must have very low latency and jitter, while some types of data traffic are more delay tolerant. In addition, business transactions must be more secure than simple Web surfing. Each of these applications requires different treatment to ensure peak performance and end-user satisfaction. The network must also have the tools to customize applications. The customization could be in how different features or functionality are combined in a single application, or allowing an end-user to change an application's GUI based on their preferences.

User awareness

The network must validate that each user is permitted to use it, understand what services the user is allowed to use, and apply each user's preferences. This enables the network to deliver end-user demanded feature functionality to an IP business phone, cell phone, PDA, or other device. The network must also understand how the user is connected and make decisions based upon this information. For example, an end-user connected to a video conference via a cell phone can only receive the audio portion, a DSL or cable user can receive audio and a single video feed, and ultra-broadband users can receive audio and a separate video window for each participant.

Network awareness

The network must be able to determine if it has the resources to allow a requested session, allow it in a "degraded" mode, or disallow the session altogether. For example, an international voice call may be allowed even if it does not meet the SLA criteria for latency, but may be disallowed if the only available path is across the public Internet. In addition, the network must have the intelligence and openness to easily and rapidly integrate and offer third-party applications or content across the network.

Nortel Networks believes in the concept of network transformation. This entails a change in both the network and the service provider business models that will lower costs, improve service, increase control, and ultimately deliver a new class of IP-enabled services that eclipse today's services the way digital eclipsed analog. The transformed network will be highly scalable, easily configurable, readily manageable, intelligent, and efficient. The key to accomplishing these enhancements lie in the themes we have highlighted: network convergence, carrier grade performance, and service intelligence. These steps will yield a network asset that can be quickly deployed to enable the value-rich, IP-enabled services that will revolutionize the United States' communications landscape.